(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number
WO 01/17288 A1

(51) International Patent Classification[7]: H04Q 7/22

(21) International Application Number: PCT/EP00/07692

(22) International Filing Date: 7 August 2000 (07.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9920323.4 28 August 1999 (28.08.1999) GB

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: FORDE, Brian, J.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). WEINMANN, Paul, C.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: TANGENA, Antonius, G.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

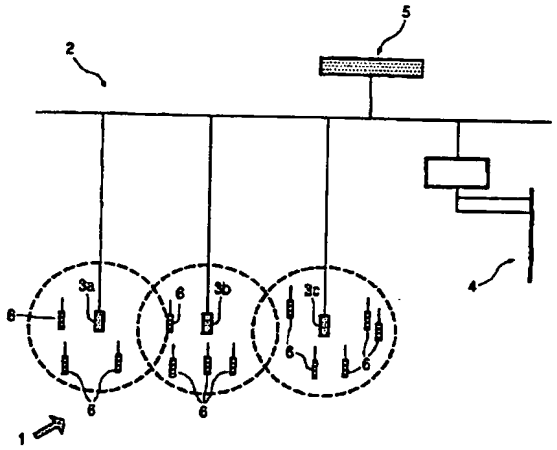
(81) Designated States *(national)*: CN, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD OF COMMUNICATING ENCRYPTED GROUP BROADCAST MESSAGES



(57) Abstract: A broadcast system for communicating single or multiple encrypted broadcast messages in a telecommunications system (1) is provided, where the telecommunications system has at least one fixed terminal (2) for communication with one or more portable terminals (6). The broadcast system includes means for transmitting first messages from the or each fixed terminal (2) for reception by portable terminals (6) in the reception area of that fixed terminal, the first message including information that specifies a channel, selected for that fixed terminal, which will be used to convey an associated broadcast message. A control means is provided for causing the or each portable terminal to receive on the specified broadcast message channels. The transmitter means then transmits from the fixed terminal (2) the encrypted broadcast messages on the said specified broadcast channels for reception, decryption and reproduction of a broadcast message, such as an audio broadcast message, by the or each portable terminal (6).

WO 01/17288 A1

DESCRIPTION

SYSTEM AND METHOD OF COMMUNICATING ENCRYPTED GROUP BROADCAST MESSAGES

The present invention relates to a system and method for communicating an encrypted broadcast message over a telecommunications system to a plurality of subscriber terminals and in particular to a system and method that allows the broadcasting of information to a plurality of wireless portable terminals. The system is particularly but not essentially based on the Digital Enhanced Telecommunications (DECT) standard.

It is known to provide telecommunications systems with an audio broadcast facility of some type, depending on the requirements and the capability of the particular system. The message that is broadcast may then be received by a plurality of the system users. One basic system is noted in the English language abstract of Japanese patent application number JP-A-5-48684. The abstract relates to a cordless telephone set having a telephone master set provided with a voice recording part, a radio (transmitting) part and antenna. A plurality of slave sets are provided with an antenna, radio part, an amplifier and a speaker. A recorded voice message may then be transmitted from the master set to the slave sets.

With such an arrangement, if each slave set is provided with only a simple receiver section (radio part), the receiver section may then be required to support not only reception of the broadcast but also support the exchange of normal telephone traffic with the master set. Problems can arise if a slave set is already being used for conducting a telephone conversation. Further problems may be experienced when attempting to transmit a broadcast to particular slave sets.

Another approach to providing an audio broadcast facility to a plurality of terminals in a telecommunications system is for a base station or some other type of control unit to set up a telecommunications link with each terminal of the plurality in a manner that is conventional for the system, that is, the type

of link that is used to carry voice or data file traffic. The audio message is then broadcast by sending it over each of the links simultaneously in the same manner that the voice signal of a normal telephone conversation would be carried. Since an individual point-to-point link needs to be established with each terminal simultaneously, this can place a heavy, if not impossible demand on the system which may only be provided with resources sufficient to establish calls to a limited number of terminals at a given time. The problem may be alleviated to some extent by setting up calls to individual terminals of the plurality one by one, or to fractions of the total number of the terminals sequentially, although this will lead to a delay while a broadcast is made to each of the terminals (or fractions of the total number of terminals) for which the broadcast is intended. This may be unacceptable in certain situations and applications, especially if the welfare of personnel using the terminals is somewhat dependant on timely reception of the broadcasts.

In telecommunications systems employing wireless links to portable terminals, attempting to provide a broadcast (such as an audio broadcast) by establishing such traffic calls to a large number of portable terminals simultaneously is even more difficult. This is partly due to the limited number of channels that may be handled by a single base station and the amount of radio spectrum that has been allocated for use by such telecommunication systems. An example of one such system is a DECT compliant telecommunications system (DECT is an abbreviation for Digital Enhanced Cordless Telecommunications). DECT systems are described in the standard ETS 300 175 of which there are several parts. The standard is published by the European Telecommunication Standards Institute and is incorporated herein by reference.

In each of the above mentioned arrangements there is no safeguard to prevent an unauthorised entity receiving and interpreting the broadcasts. This may cause problems where security is an issue.

It is an object of the present invention to provide a system for the broadcasting of encrypted messages such as audio messages or data files

over a telecommunications system that allows a plurality of portable terminals to receive and decrypt the messages that are broadcast.

It is another object of the present invention to provide a system for the broadcasting of encrypted messages such as audio messages or data files over a telecommunications system and which allows a plurality of portable terminals to receive and decrypt messages that are broadcast, while at the same time making efficient use of system resources.

In accordance with a first aspect of the present invention there is provided a broadcast system for communicating a broadcast message in a cordless telecommunications system, the telecommunications system having at least one fixed terminal for communication with one or more portable terminal over an air interface, said broadcast system including: first transmitter means for transmitting a first message from the fixed terminal, the message including information specifying a channel, selected for that fixed terminal, to convey the broadcast message; control means, responsive to the first message, for instructing the at least one portable terminal to receive on the selected channel; broadcast message encryption means for encrypting broadcast messages; and second transmitter means for transmitting from the fixed terminal on the selected channel a broadcast message in encrypted form for reception and decryption by the at least one portable terminal.

The broadcast messages are typically audio or data file type messages.

The first and second transmitter means may be incorporated in the fixed terminal. Indeed the first and second transmitter means may be the same entity. The first and second transmitter means may be the same system component. The control means may be located in the portable terminal. Each of the first and second transmitter means and control means may be system applications or the like and the terms do not necessarily relate to hardware.

By broadcasting the message as a connectionless message it is possible to transmit substantially simultaneously to a plurality of portable terminals without setting up an individual call to each portable terminal and therefore without exceeding the limitations of the system.

Such a broadcast facility would be of particular use where portable terminals are being carried by security guards or medical workers, where quick substantially simultaneous broadcasting of messages or an alarm signal to personnel is important.

Preferably, the first transmitter means includes paging means to generate and include in the first message paging information specifying the identity of the at least one portable terminal for which the broadcast is intended, the control means being responsive also to this paging information such that only a portable terminal having the specified portable terminal identity will be instructed to receive the encrypted broadcast message on the selected channel. This allows broadcast messages to be directed to specific portable terminals.

The broadcast system may also be provided with assigning means for selectively assigning a portable terminal with a portable terminal identity of the type suitable for specifying by the paging means. Therefore, by assigning a number of portable terminals with a common identity, all such terminals may be instructed to receive a broadcast by including in the first message paging information specifying only that one common identity.

Preferably broadcast messages are encrypted by the broadcast message encryption means using a specific encryption algorithm and encryption key such that only portable terminals in possession of a corresponding decryption algorithm and decryption key can decrypt the received encrypted broadcast message.

A broadcast message may be provided with an identifier which is included in the first message. In this case, the identifier may be used by a portable terminal receiving an encrypted broadcast message to select an appropriate decryption algorithm and / or decryption key.

If the cordless telecommunications system is a DECT based telecommunications system then the assigning means may selectively assign a portable terminal with a portable terminal identity which is a Temporary Portable User Identity (TPUI).

If the telecommunications system is based on the DECT standard, or a modified form of the DECT standard, the specified broadcast channel may be a DECT physical channel which may then be used to support a DECT simplex bearer. The specified channel can be used to support a connectionless downlink bearer. This has a particular advantage in a DECT compliant system, as the applicants have recognised, since the DECT standard allows for connectionless communications to be set up from the radio fixed parts of the fixed terminals to the portable parts although these connectionless communications are normally only used to carry system information and other control information.

In accordance with a second aspect of the present invention there is provided a method for communicating a broadcast message in a cordless telecommunications system having at least one fixed terminal for communication with one or more portable terminal over an air interface, said method comprising the steps of: transmitting a first message from the fixed terminal, the message including information specifying a channel, selected for that fixed terminal, to convey the broadcast message; instructing the at least one portable terminal to receive on the selected channel; encrypting broadcast messages; and transmitting from the fixed terminal on the selected channel a broadcast message in encrypted form for reception and decryption by the at least one portable terminal.

Multiple instances of broadcast messages may be established to allow the presence of multiple at least partially overlapping broadcast messages. Such broadcasts may allow multiple streams of information to be broadcast to a plurality of wireless portable terminals.

In accordance with a further aspect of the present invention there is provided a communications device apparatus having the technical features of the first transmitter means in the broadcast system.

In accordance with a yet further aspect of the present invention there is provided a communications device apparatus having the technical features of the control means in the broadcast message system.

In accordance with a yet further aspect of the present invention there is provided a communications device apparatus having the technical features of the second transmitter means in the broadcast message system.

In accordance with a yet further aspect of the present invention there is provided a communications device apparatus having the technical features of the broadcast message encryption means.

In accordance with a yet further aspect of the present invention there is provided a communications device apparatus having the technical features of the portable terminal usable in conjunction with the broadcast system for reception and decryption of a broadcast message.

Other aspects and optional features of the present invention appear in the appended claims, to which reference should now be made and the disclosure of which is incorporated herein by reference.

The present invention will now be described by way of example only with reference to the accompanying drawings in which:

Figure 1 shows a schematic representation of a telecommunications system incorporating the present invention;

Figure 2 shows an overview of an encryption / decryption process; and

Figure 3 shows schematically components of a system suitable for generating an encryption key.

The particular communications system shown in Figure 1 is based on a DECT compliant cellular communications system 1 in which the fixed terminal takes the form of a DECT fixed part (FP) 2 which includes a plurality of radio end points in the form of DECT radio fixed parts (RFP's) 3. Three such RFP's 3a, 3b, 3c are shown.

Although the present system is based on a DECT compliant system, the present system is provided with various features which fall outside the scope of the current DECT base standards. Such features will be highlighted where appropriate, but for the purpose of understanding the present invention,

references to 'DECT compliant' or 'DECT' when discussing particular features should be taken to indicate normal DECT functionality unless otherwise stated.

The RFP's 3 are networked together and FP 2 is connectable via an interface to external telecommunication networks such as the public switched telephone network 4 although this is optional. The FP also includes a control unit 5 which serves to control the general operation of the whole system including the interoperability of the RFP's 3 with each other. The control unit 5 may also be provided with private automatic branch exchange (PABX) functionality. Although a number of RFP's 3 are used to form a multi cell system, it is possible to provide a single cell system which uses only one RFP 3. In a DECT compliant system a portable terminal takes the form of a portable part (PP) 6 which is capable of establishing communication with the fixed part by establishing a wireless link with a RFP 3a, 3b, 3c. This allows the exchange of traffic such as voice or data, as is well known to the person skilled in the art. Although twelve PP's are shown other numbers may be used. The wireless link communication between an RFP and a PP is provided by so-called bearers which are established on one or more DECT physical channels (channel). Each channel is created by transmitting on one particular slot on one particular radio frequency (RF) in successive time division multiple access (TDMA) frames.

As stated above, a DECT communications system may be provided with one RFP 3 or a number of RFP's 3. Obviously, if the system has only one RFP 3 then this RFP must cater for all connections that are established with the PP's 6. However, in the case of a system having a plurality of RFP's 3, (as is the case for the system illustrated in Figure 1), provided for the purpose of increasing system capacity and/or coverage area, connections are established between RFP's 3 and PP's 6 depending on the available link quality, which usually though not always results in a link being established between the PP 6 and the nearest RFP 3.

Before the PP6 can participate in traffic communication with the fixed system it needs to attain a condition where it is synchronised with a RFP 3 of the FP 2. This is made possible in a DECT system because each RFP 3

maintains transmissions that carry information relating to the identity of the particular RFP 3 and the FP 2 it is connected with together with other system information. Because each RFP 3 is always transmitting such information a PP 6 is able to receive on each DECT system channel in turn and to monitor for activity on those channels.

This transmitted information is called N-channel and Q-channel information as will be understood by the person skilled in the art. For the purpose of clarity it should be mentioned that the DECT N-channel and DECT Q-channel are logical channels and not DECT physical channels.

Because it is the responsibility of the PP 6 to detect the presence of any nearby RFP's 3, when a PP 6 is activated it begins to listen on each DECT channel for N-channel and Q-channel information broadcast by the RFP's 3. If a given RFP 3 is not involved in supporting a traffic connection with a PP then this information is broadcast by itself on a so-called dummy bearer. If a given RFP 3 is involved in supporting one or more traffic connection with one or more PP's 6, the RFP 3 broadcasts this information on each traffic bearer. A RFP 3 supporting at least one traffic connection may drop the dummy bearer although the broadcast of the N-channel and Q-channel information on the dummy must be restored if all traffic connections with that RFP 3 cease. In any case a RFP 3 will always be transmitting N and Q-channel information on at least one DECT channel. The dummy bearer is not intended for reception by a particular PP 6 but is merely for making RFP 3 identity and system information available all of the time to any in-range PP's 6 that happen to be in the vicinity.

When a PP 6 is initially switched on, it listens out for the presence of an in-range RFP 3 by scanning through all the valid DECT channels until if finds one with some activity. If the RFP 3 is indeed already supporting a voice or data call to one or more other PP then so-called traffic bearers are already established between the RFP 3 and those PP's and the system information will be found in these. This is sufficient to service the PP 6 with the system information that it needs to synchronise with the RFP 3 and be in a condition ready to make or receive calls to it. If however the RFP 3 is not supporting any

voice or data calls there will be no traffic bearers and hence PP's 6 in the vicinity of the RFP 3 rely on the so-called dummy bearer transmitted by the RFP 3 at regular intervals on one of the valid DECT channels so that the PP's may synchronise with this.

The PP 6 sets up a so-called synchronisation bearer on the various DECT channels to determine if a nearby RFP is indeed transmitting on that channel. If it is established that this is not the case, a synchronisation bearer is set up on a different DECT channel until a channel is found that is carrying N-channel and Q-channel information. Setting up a synchronisation bearer allows any N-channel and Q-channel information on a DECT channel to be read. This information is used by the PP 6 to determine if it has access rights to the fixed part, and if it does, the PP 6 enters a state in which it is ready to make and receive calls.

A traffic bearer, as is normally used for voice or data communication, operates in a connection oriented mode since it involves the three stages of setting up a connection from one source to one or more destination, transferring data, and finally releasing the connections. In contrast, a dummy bearer operates in a connectionless mode, since it involves the transmission of self contained units of data from one source to one or more destination. A further type of bearer exists and is called a connectionless bearer. It is similar to a dummy bearer, except that while a dummy bearer can only carry system information, the connectionless bearer can carry other types of information. Further information on the nature of these different bearers is given in the above mentioned DECT standard and will not be reproduced herein unless relevant to understanding of the present invention.

Since all types of bearer contain RFP and system information in the form of N-channel and Q-channel information, all PP's in range of and synchronised with a RFP, whatever their present state (for example, engaged with a voice call or in an idle condition), receive and have access to this information. Another type of DECT logical channel is called the P-channel which contains paging information from the RFP to the PP. When paging information is transmitted, it also appears on all bearers. Therefore any PP

which is able to receive N-channel and Q-channel information will also be able to receive any transmitted P-channel information. Because all synchronised PP's always hear any P-channel information that is transmitted, information is carried on this channel to instruct a particular PP which channel to receive on.

In order to broadcast a message such as an audio message or data file to a particular PP, that PP is first invited to receive on a particular DECT channel that will be used as the broadcast channel for carrying the broadcast information. Once the PP is receiving on that channel the message is transmitted on that channel for reception by the PP. By inviting a plurality of DECT PP's to receive on that channel, all of those PP's will then be able to receive the broadcast message.

A connectionless downlink bearer is set up by each RFP on the broadcast channel, which may be different for each RFP. All PP's in range of a RFP are now capable of receiving the broadcast message simultaneously if they listen to the channel selected on that RFP for carrying the connectionless downlink bearer. As stated above, a connectionless bearer is similar to a dummy bearer, but in this case the connectionless bearer has it's B-field filled with information relating to the broadcast message itself, as will be understood by the person skilled in the art. Although the message may contain voice or data file information, other types of information could be broadcast such as information representing an alarm signal. It is noted that this is in contrast to the concept of establishing a traffic bearer to each in-range PP for which the broadcast message is intended and relaying the message over these traffic bearers. A DECT RFP cluster is only capable of supporting a limited number of traffic bearers and there is an absolute number of traffic bearers that may be established in a DECT system anyway before frequency reuse becomes necessary. Therefore, by employing a connectionless bearer for carrying the broadcast message, a plurality of PP's may receive the message without unduly loading the telecommunications system.

In order for a given PP to actually receive and reproduce the broadcast message, a first message containing information telling the PP's which DECT channel is being used for the broadcast message is transmitted by each RFP

on all bearers as a short page message. The short page message which is transmitted on the P-channel is used to identify the DECT channel that will carry the broadcast message. Short page messages are normally carried in the A-field, as will be known to the person skilled in the art.

In practice, if a dummy bearer is in use by a particular RFP, it is preferable to convert the dummy bearer into a connectionless downlink bearer for carrying the broadcast message thus claiming the DECT channel previously used for carrying the dummy bearer, rather than to set up a connectionless downlink bearer on a different DECT channel. One reason for this preference arises because if a given RFP is transmitting only a dummy bearer, any PP's synchronised with that RFP will be receiving on the DECT channel carrying the dummy bearer. This will generally avoid the need to instruct a PP to receive on a different DECT channel.

Now taking the example of providing a second broadcast message while the first broadcast message is being transmitted, the second broadcast message is provided by setting up a second connectionless downlink bearer from each RFP. For a given RFP, the second connectionless downlink bearer will be on a DECT channel different to the first connectionless downlink bearer. The B-field of the second connectionless downlink bearer is filled with information relating to the second broadcast message itself, as will be understood by the person skilled in the art.

In order for a given PP to actually receive and reproduce the second broadcast message, a further instance of first message is generated which contains information telling the PP's which DECT channel is being used for the second broadcast message. This further instance of first message is transmitted by each RFP as a short page message on all existing bearers. As stated above, because the short page messages are carried on the P-channel they can be present and are normally contained in all bearers and are normally carried in the A-field. This results in all PP's hearing the short page messages which notifies them of the existence of a broadcast. A PP can then receive on the DECT channel carrying the second connectionless bearer, and therefore the second broadcast message, to reproduce the second broadcast message.

It is possible to provide further instances of broadcast messages in the same way that the second broadcast message is provided, each broadcast message having an associated first message. Because each broadcast message may be performed independently of the others, it is possible to provide multiple overlapping simultaneous broadcast messages in the system. It is noted that the second and further connectionless downlink bearers are unlikely to be set up by converting the dummy bearer into one of these connectionless downlinks, since the dummy will have normally been converted into the first connectionless downlink bearer.

By 'simultaneous' it is meant that more than one broadcast message may be provided at the same time. Since each broadcast message is unrelated and independent of any other broadcast message there is no such requirement that the broadcast messages are to be synchronised with each other or necessarily performed at the same time.

The above described mechanism of providing a single broadcast message in a DECT telecommunications system would appear to comply with the current DECT standards. However, the presently described mechanism of providing second and further instances of simultaneous broadcast messages by adding second and further connectionless downlink bearers, respectively, requires a departure from the current version of the DECT base standards. According to the standards, for each cluster of cells only one instance of connectionless message control downlink service may exist. Connectionless message control (CMC) relates to the functions that control and distribute the information of all connectionless services to one or more connectionless bearer control, as will be understood by the person skilled in the art. Although each CMC allows a maximum of two connectionless bearers, the second is only intended for channel hopping purposes and the data on each bearer is exactly the same. Therefore, second and further broadcast calls carried on second and further connectionless downlink bearers require second and further instances of CMC respectively.

The presence of second and further instances of CMC does not affect the normal operation of a DECT based system. This means that it is possible

to use an unmodified PP with the telecommunications system, although such a PP would not be able to receive broadcast calls.

It is not always a requirement for all PP's to receive a broadcast message and it is possible to cause a given broadcast message to be received by only one of the PP's or a selection of the PP's. PP's may be assigned an identity or group identity, and only those PP's carrying that particular identity may elect to receive a given broadcast. This may be achieved in a DECT system by assigning a Group Temporary Portable User Identity (TPUI) to a portable part, or a group of portable parts so that only those PP's having a particular TPUI are invited to receive the broadcast message. More than one TPUI may be employed in the system thus allowing different groups of PP's to be created and independently selected for receiving a broadcast. The TPUI related information is also present in the P-channel and is carried in the short page message, so again, all PP's are capable of receiving this information. The use of identities and addressing will be known to the person skilled in the art and further information is contained in the DECT standards. Throughout the description, a reference to a TPUI should be read as a reference to a connectionless group TPUI unless the context suggests otherwise. An example of where this is not the case would be a reference to an individual TPUI, as will also be understood by the person skilled in the art.

The MAC layer information in the short page message contains the location of the connectionless bearer, i.e. in terms of time slot and frequency. This may be different for each RFP. The short page message may originate from an application in the RFP. In particular the short page message contains information present in the P-channel; that is the identity of the PP's which should receive the broadcast message, and the DECT channel the broadcast is transmitted on.

The broadcast message may originate from anywhere in the system and for example may originate from the PSTN or from another PP. In the latter case the message is transmitted from the PP to an in-range RFP over a normal traffic bearer, after which the message is broadcast to the other PP's by the mechanism described above. The originator of the broadcast message

The broadcast group identities (which are group TPUI's in the specific example) can be assigned to a PP just after the PP has subscribed, or at location registration when the individual TPUI is assigned. Alternatively, the identity could be assigned at any time since it is permitted to re-arrange a PP into different groups at any time. A PP can be a member of multiple groups.

Now that a mechanism has been described for providing single and multiple broadcast calls in a DECT-based telecommunications system, the encryption related operations will now be described, with reference to Figures 2 and 3.

With reference to Figure 2, before broadcast messages are transmitted from the fixed terminal, they are encrypted by broadcast message encryption means 11. The encryption means employs an encryption algorithm 12 and an encryption key 13. A non-encrypted message (a so-called 'plaintext' message) 30 is input to the encryption means 11 and the broadcast encryption means 11 operates on the non-encrypted message 30 to convert it into an encrypted broadcast message 40 (a so-called ciphertext message). It is this encrypted message 40 which is broadcast over the air interface from the fixed terminal 3 to the portable terminals 6. Because the broadcast message is encrypted, any unauthorised interception of the message will not allow the content of the message to be readily deciphered.

If the broadcast message is received and subsequently decrypted, the original content of the message may be recovered and reproduced. Those portable terminals for which the broadcast message is intended are therefore provided with broadcast message decryption means 21. In order for the decryption means 21 to convert a received encrypted message 40 into the original non-encrypted message 30, the decryption means 21 requires a specific decryption algorithm 22 and specific decryption key 23. The specific decryption algorithm 22 and specific decryption key 23 are associated with the encryption algorithm 12 and encryption key 13 that were originally used to encrypt the broadcast message. Only the correct decryption algorithm 22 and correct decryption key 23 will allow the broadcast message decryption means 21 to decrypt the message correctly. By providing a suitable form of algorithm

and a large number of possible decryption keys, it is very difficult to perform a successful decryption operation on an encrypted message without possessing the correct decryption algorithm and decryption key for that message. By this mechanism, a message may be broadcast with the knowledge that it will be comprehended readily only by intended recipients.

For the above mentioned encryption system to work effectively, there needs to be a procedure in place to provide the intended recipients of the broadcast message (the portable terminal) with the correct decryption algorithm and decryption key. There are a number of possible ways to do this, some of which will now be discussed, first in general terms and secondly in a telecommunications system based on a DECT-compliant telecommunications system.

One way is to provide a portable terminal with a specific decryption algorithm and specific decryption key during manufacture. Another way is to provide a portable terminal with a specific decryption algorithm and specific decryption key that is normally fixed but may be modified if necessary by the user or a system administrator. In this case the key and algorithm are transferred to the portable terminal via a physical link established with a programming unit or equivalent. The unit may take the form of a cradle. It is important that the link is a physical one and not a link established over the air. In both cases, by providing the fixed terminal with the necessary information about the portable terminal including the specific decryption algorithm and specific decryption key, the fixed terminal can generate an encrypted broadcast message that may be received and decrypted by the said portable terminal. Advantages of this system include: 1) the decryption process is transparent to the user of the portable terminal so the user is not required to take any action; 2) the decryption algorithm and key are hidden in the portable terminal and therefore are not readily accessible; 3) a portable terminal may be provided with an identifier relating to the in-built algorithm and key allowing a plurality of portables bearing the same identifier to be selected, and since each has the same decryption algorithm and decryption key, a group may be formed which is capable of decrypting the same encrypted broadcast message. An

may specify the group for which the broadcast is intended by forwarding the appropriate TPUI information. In one example this may be generated by the user indicating the intended recipients by entering information via the keypad of the PP.

Each RFP ensures the quality is maintained of each connectionless downlink bearer currently in use. Connectionless bearer hopping may be employed to change to another DECT channel if channel quality is poor. A short page message can be used to inform PP's synchronised with the RFP of the new channel carrying the connectionless bearer. When the connectionless bearer is moved to a different channel, a new page is sent out regularly to inform all of the in range PP's of this. Furthermore, for a given broadcast message, it's associated connectionless downlink bearer will not necessarily be on the same DECT channel for each RFP, so short page messages specifying the location of the connectionless downlink bearer and the broadcast call TPUI information will be sent out regularly by each RFP for the entire duration of the broadcast message. This will allow PP's to roam into a cell served by a different RFP which may well be transmitting the connectionless downlink for a given broadcast message on another DECT channel, and still receive the broadcast message if necessary by receiving on that channel. It also allows a PP which is activated only during a broadcast to begin receiving the broadcast. Connectionless bearer handover could also be implemented in other ways although this may violate the DECT standard.

Optionally a number of TPUI's may be used, each having a priority value assigned. Where priority values are employed, a PP can be set to receive or reject a broadcast call depending on the priority value associated with the broadcast.

A given PP may have a number of identities assigned to it. Furthermore, if a given PP is instructed to receive more than one broadcast message simultaneously a signal could be generated by the portable part alerting the user to switch to a different broadcast. The user could be alerted, for example by an audio tone or a display message. Alternatively, if the broadcast message is of data, an application on the portable part could

automatically switch to a different one of the broadcast calls. Each broadcast message may be assigned a priority value allowing the PP to alert the user of the PP depending on the priority value of the message. Furthermore, the PP may automatically switch to receive the broadcast message having the highest priority value. A priority value could be reserved for indicating an emergency status in which case any broadcast having such an assigned priority value will be received and reproduced by portable parts irrespective of whether they are already supporting a broadcast or normal connection based call.

A given PP could receive more than one broadcast message simultaneously. This would allow an audio broadcast, for example, to be reproduced, while a further audio broadcast could be stored. Other combinations of received broadcasts include audio and data and audio and video broadcasts.

If a PP is already being used for a normal connection based call, the occurrence of a broadcast to that terminal can have a number of effects. For example, a signal could be generated by the portable part alerting the user of the broadcast allowing the user to switch to the broadcast or ignore it. The user could be alerted, for example, by an audio tone or a displayed message. If the user chooses to accept the broadcast, the normal connection based call may be put on hold. Alternatively, the portable part could automatically switch to reproduce the broadcast, perhaps also putting the normal call on hold. The automatic switch could be implemented so that it only occurs if broadcasts have specified associated priority values. A PP may be provided with means for reproducing a audio broadcast call at a volume which is greater than that employed during a normal connection based call. For this purpose a loudspeaker may be provided in the portable part which may be activated automatically. As stated above, the broadcast could be representative of an alarm signal. Such a broadcast could be initiated by a user of a PP activating an alarm function provided on the PP.

The control unit sends a broadcast message to all RFP's containing the group TPUI and which broadcast messages are to be transmitted by the RFP's.

extension of this system is to provide a portable terminal with a plurality of decryption algorithm and decryption key pairs which may be selected as appropriate, either automatically within the portable terminal or by intervention of the user. A disadvantage of this system is that the decryption key and decryption algorithm may not be re-programmed which can result in an inflexible system and cause security problems if a portable terminal is acquired by an unauthorised person. In a DECT based telecommunications system such an algorithm and key may be provided by passing the group TPUI's and SCK's / DCK's to the PP via an electrical connection (for example a serial link). This contributes towards the security of the system because the information is not transmitted over the air interface.

Another way is to provide portable terminals with one or more standard decryption algorithm but to use individual encryption keys at the fixed terminal and corresponding individual decryption keys at the portable terminal, where the individual keys may be changed. The broadcast messages are encrypted taking into account the decryption algorithm and key held in the or each portable terminal for which the broadcast is intended. The key may be input by the user of the portable terminal, or generated from information input by the user of the portable terminal. This system has the advantage that the key can be changed when required simply by informing the user (via a secure channel) of the new key, or information required to generate the new key, that is required for correct decryption. In some cases the required key can be generated from a combination of information input by the user and information associated with the portable terminal itself, for example an equipment serial number. The information input by the user may be stored for a duration which conveniently allows the user to receive broadcast messages without the necessity to input information each time a broadcast occurs.

In a DECT based telecommunications system a received encrypted broadcast message could be decrypted using the key stream generator together with a decryption key in the form of a static cipher key (SCK) as will be understood by the person skilled in the art. The SCK itself may be input by the user of the DECT portable part or be generated from information input by

the user, thereby allowing a reduced amount of information to be input by the user. The SCK may be generated from a combination of information such as the portable terminal's IPUI (International portable user identity) or IPEI (International portable equipment identity) and information input by the user. This offers the advantage of allowing less user information to be input while at the same time increasing the security of the encrypted broadcast, since knowledge only of the information input by the user will not allow generation of the required SCK. A disadvantage of the latter system is that encrypted group broadcasts cannot be made since each portable terminal will have a different IPEI and IPUI leading to the generation of different SCK's in each portable terminal.

Another way is to provide each portable terminal with one or more selectable decryption algorithm and to generate the decryption key internally. In this case it is necessary for the portable terminal to generate a decryption key that is suitable for decrypting the broadcasts that are received. Likewise it is necessary for the fixed terminal to use an encryption key and algorithm such that the broadcast encrypted message can be decrypted by the or each appropriate portable terminal. By providing a way for a specific portable terminal to generate a particular decryption key on the command of the fixed terminal, a powerful and secure broadcast message system is possible. Furthermore, if a portable terminal can be so commanded by the fixed terminal over a non-secure channel without appreciably compromising security, the system is also convenient to use.

This may be implemented in a DECT based telecommunications system as an extension of the process for authentication of a portable part. With reference to Figure 3, a DECT fixed terminal (Fixed Part, FP) is able to authenticate a DECT portable terminal (Portable Part, PP) to establish that a portable part is one that it claims to be. Authentication involves the use of a cryptographic challenge-response mechanism wherein the FP challenges a PP to perform a calculation and present a result. The FP also performs the same calculation and if the result generated by the PP matches the (expected) result generated by the FP, the FP accepts the PP as being genuine. The result

generated by the PP is denoted as 'RES1' which is produced by authentication processes A11 and A12. The inputs to the processes are 'K', an authentication key, 'RS', a value used to establish authentication session keys and 'RAND F', a random value. The value RS and RAND F are issued by the FP and broadcast over the air interface to the PP. The FP is also provided with authentication processes A11 and A12. Because the FP knows what the value of K is for the genuine PP it is attempting to authentic, and also knows RS and RAND F, the FP can calculate locally the expected value of RES1. The PP calculates the value RES1 and transmits it back to the FP over the air interface and if the value matches the locally calculated value this indicates that the PP is genuine. This process allows the PP to demonstrate it's knowledge of the correct value of K without disclosing the value over the air.

Another product of the authentication process A11 and A12 is a so called Derived Cipher Key (DCK). A new DCK is generated on each occurrence of authentication. Authentication occurs at the beginning of a call but may be invoked at any time during a call. When a DECT PP receives an encrypted broadcast call, this may be decrypted using the key stream generator together with the correct DCK, rather than the SCK as described above.

It will be apparent that a number of PP's may be provided with the same DCK by ensuring that each PP performs the same authentication process A11 and A12 on the same values of K, RS and RAND F. If each of the number of PP's is provided with the same DCK this means that a group broadcast could be received and decrypted by these PP's. In order to maintain security of the broadcasts, K is generated from authentication code AC via authentication key stream process B1. The authentication code in input by the user of the PP.

Whichever method is selected for providing a portable with the required decryption algorithm and decryption key pair, each portable terminal may be capable of possessing a plurality of such pairs. Furthermore, irrespective of whether the algorithm and / or key is selected automatically by an application in the portable terminal or selected or input by a user, there can be a requirement that the correct pair is applied to a particular broadcast message,

especially where there are multiple broadcasts present, or broadcasts requiring different privileges for access. To allow for this each broadcast message carries an identity allowing the correct pair to be selected and applied to it. For example, at a basic level, a portable terminal could indicate in a display that an incoming broadcast message carries identity number 1. The user would note this information and input the correct decryption key for messages carrying such identity numbers. Users not authorised to receive messages carrying such an identity number would not be provided with the correct decryption key. In a system where user intervention is undesirable, an application in the portable terminal would note the message identity number and apply the correct decryption key automatically. A portable terminal not authorised to receive messages carrying such an identity number would not be provided with the correct decryption key. Identity numbers could also be used to indicate or select the appropriate decryption algorithm.

In a DECT based encrypted broadcast system, such a broadcast message identifier may be carried in the first message together with the group TPUI information. One way to implement this is by use of the <<PORTABLE IDENTITY>> information element. This element is normally used to transport the DECT portable identity during paging. Octet 3 of the element is used to indicate the identity type coding for portable identities. When octet 3 indicates that the identity is a temporary portable user identity (TPUI), the actual TPUI value is contained in octets 5, 6 and 7. However, bits 8, 7, 6 and 5 of octet 5 are always set to zero. Therefore these bits are employed in this implementation to indicate the identity of the broadcast message and since four bits are available, a maximum of 16 different broadcast messages may be identified, although this is not to be interpreted as limiting the scope of the present invention. The use of these bits for providing a broadcast message identity may possible deviate from the teaching of the DECT base standards.

Such identity information can be especially beneficial in those systems which, like a DECT based telecommunication system, may assign a different group TPUI to a PP as it roams from one cell to another. Through the use of a broadcast identity, a PP can roam into another cell and continue to receive

and decrypt a broadcast message despite a different TPUI being used. This is because the broadcast identity may be used by the PP to determine which broadcast message it is receiving and therefore which decryption key and algorithm to use.

Other ways of providing a portable terminal with decryption keys and algorithms may be employed although they may offer a lower standard of security. For example, the decryption key could be the group TPUI itself, a function of the group TPUI, a key that is broadcast in the first message, or a key based on the user authentication key. It will be appreciated by the person skilled in the art that some of these techniques will be more suitable for broadcasts to individual portable terminals rather than groups of terminals and vice versa. A DCK could be associated with a group TPUI. Indeed a PP may hold several DCK's associated with many group TPUI's. In one specific example, if a second group call is in the process of being set up while a first group call is in the process of being received by a PP, the PP receives a short page message, informs the user of the call and the user may decide whether listen to the second call. If the user decides to listen, a the DCK associated with the group call is loaded into the encryption algorithm and the MAC is set to listen to the correct slot and frequency of the second connectionless bearer. The received B-field data is then decrypted.

In order to inform a portable terminal of the fact that a broadcast message is encrypted, the connectionless broadcast message could carry information which marks the message as being encrypted. If the broadcast system is based on a DECT telecommunications system, this may be done by transmitting a MAC control encrypt start request message periodically on the bearer itself.

This application is related to our co-pending UK patent applications number GB9920325 entitled 'Broadcast Facility' and number GB9920324 entitled 'Multiple Broadcast Facility'.

While the present invention is described in some detail with reference to a DECT compliant telecommunications system carrying modifications, it is noted that the invention could be implemented in other telecommunication

systems capable of establishing single or multiple instances of encrypted connectionless messaging. In this case portable terminals are instructed to receive the messages using a form of addressing different to DECT TPUI addressing. That is, the target audience of the call is defined by a group identity, which may be programmable for each portable terminal. Details of the encryption mechanism will likely differ from those described above with reference to a DECT-based system.

From reading the present disclosure, other modifications will be apparent to persons skilled in the art. Such modifications may involve other features which are already known in the design, manufacture and use of systems and devices and component parts thereof and which may be used instead of or in addition to features already described herein.

CLAIMS

1. A broadcast system for communicating a broadcast message in a cordless telecommunications system (1), the telecommunications system having at least one fixed terminal (2) for communication with one or more portable terminal (6) over an air interface, said broadcast system including:

first transmitter means for transmitting a first message from the fixed terminal (2), the message including information specifying a channel, selected for that fixed terminal, to convey the broadcast message;

control means, responsive to the first message, for instructing the at least one portable terminal to receive on the selected channel;

broadcast message encryption means (11) for encrypting broadcast messages; and

second transmitter means for transmitting from the fixed terminal (2) on the selected channel a broadcast message in encrypted form for reception and decryption by the at least one portable terminal (6).

2. A broadcast system in accordance with claim 1 wherein the first transmitter means includes paging means to generate and include in the first message paging information specifying the identity of the at least one portable terminal (6) for which the broadcast is intended, the control means being responsive also to this paging information such that only a portable terminal (6) having the specified portable terminal identity will be instructed to receive the encrypted broadcast message on the selected channel.

3. A broadcast system in accordance with claim 1 or 2 and further including assigning means for selectively assigning a portable terminal (6) with

a portable terminal identity of the type suitable for specifying by the paging means.

4. A broadcast system in accordance with claim 1, 2 or 3 and further including message decryption (21) means provided in each at least one portable terminal, the message decryption means employing a decryption algorithm (22) and decryption key (23).

5. A broadcast system in accordance with claim 4 and further including means for providing the decryption means (21) with a decryption algorithm and/or a decryption key.

6. A broadcast system in accordance with claim 4 or 5 wherein a broadcast message is encrypted by the broadcast message encryption means (11) using a specific encryption algorithm (12) and encryption key (13) such that only portable terminals in possession of a corresponding decryption algorithm (22) and decryption key (23) can decrypt the received encrypted broadcast message.

7. A broadcast system in accordance with any one of claims 1 to 6 wherein the broadcast message has a message identifier, the message identifier being included by the first transmitter means in the first message.

8. A broadcast system in accordance with claim 7 when appended to claim 4, 5 or 6 wherein the decryption means (21) is responsive to the message identifier to select a decryption algorithm and / or decryption key.

9. A broadcast system in accordance with any one of claims 1 to 8 wherein the cordless telecommunications system (1) is a DECT based telecommunications system and the broadcast message channel is connectionless.

10. A broadcast system in accordance with claim 9 when appended to claim 2 or 3 wherein the portable terminal identity of the at least one portable terminal (6) is specified or assigned, respectively, using a temporary portable user identity (TPUI).

11. A broadcast system in accordance with claim 9 when appended to claim 7 or 8, wherein the identifier is a value transported in the <<PORTABLE IDENTITY>> information element and located at bit 8, 7, 6 and 5 of octet 5 when octet 3 indicates that the identity type coding is a temporary portable user identity (TPUI).

12. A broadcast system in accordance with claim 4 when appended to claim 3 wherein the decryption key (23) is derived from the portable terminal identity.

13. A method for communicating a broadcast message in a cordless telecommunications system (1) having at least one fixed terminal (2) for communication with one or more portable terminal (6) over an air interface, said method comprising the steps of:

transmitting a first message from the fixed terminal (2), the message including information specifying a channel, selected for that fixed terminal, to convey the broadcast message,

instructing the at least one portable terminal (6) to receive on the selected channel;

encrypting broadcast messages; and

transmitting from the fixed terminal (2) on the selected channel a broadcast message in encrypted form for reception and decryption by the at least one portable terminal (6).

14. A method in accordance with claim 13 and further comprising the steps of:

generating and including in the first message paging information specifying the identity of the at least one portable terminal for which the broadcast is intended, such that only a portable terminal (6) having the specified portable terminal identity will be instructed to receive the encrypted broadcast message on the selected channel.

15. A method in accordance with claim 14 and further including the step of selectively assigning a portable terminal (6) with a portable terminal identity.

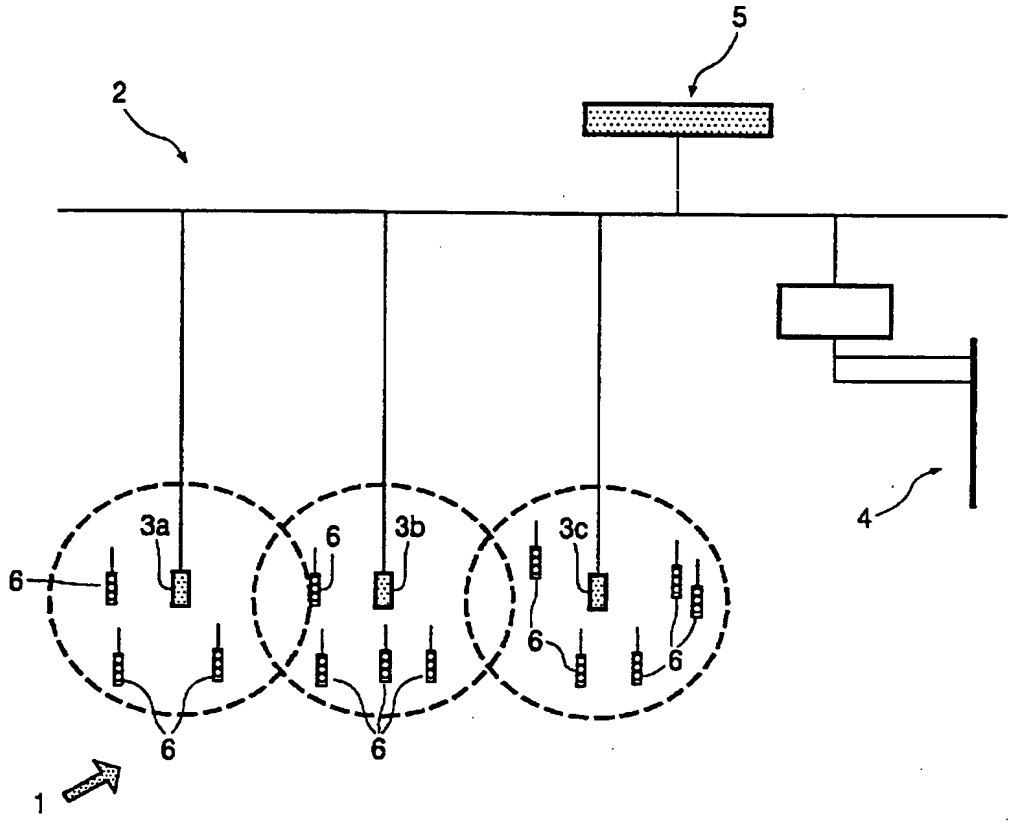


FIG. 1

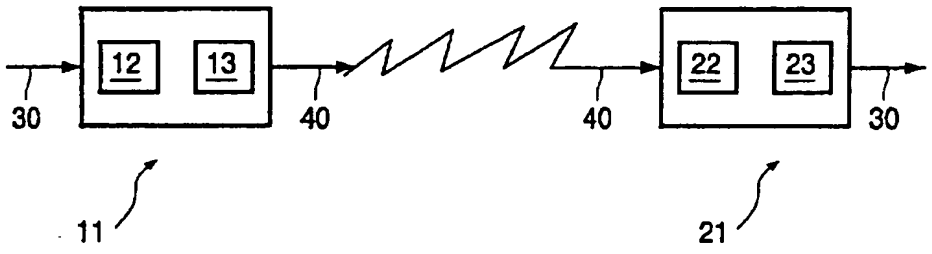

12
13
22
23
30
40
40
30
11
21

FIG. 2

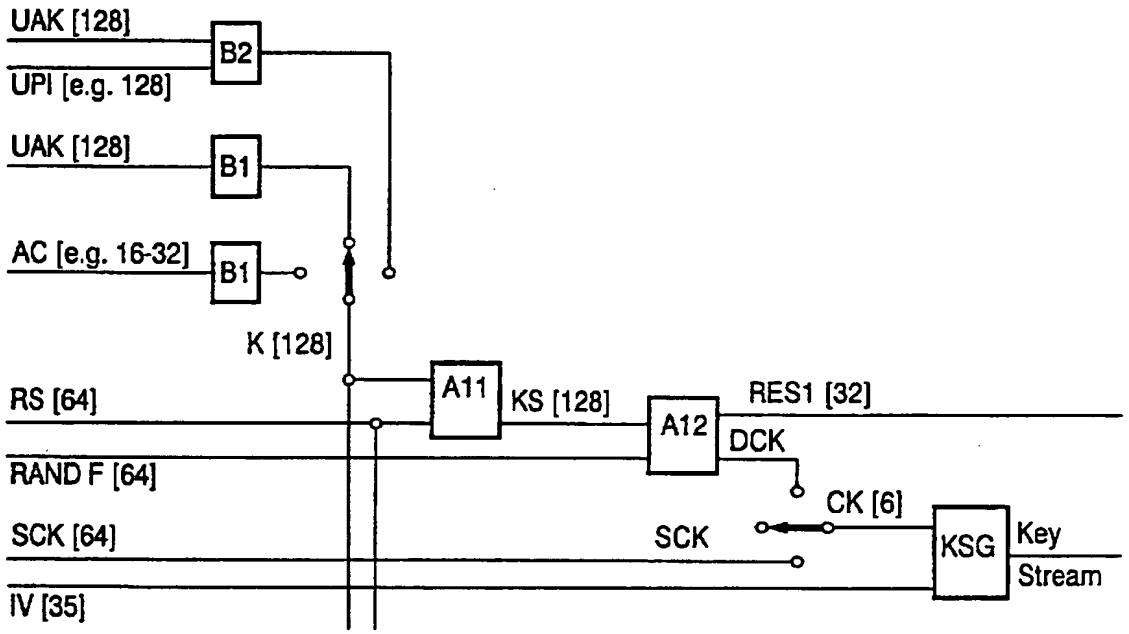

UAK [128]
B2
UPI [e.g. 128]
UAK [128]
B1
AC [e.g. 16-32]
B1
K [128]
A11
KS [128]
A12
RES1 [32]
RS [64]
DCK
RAND F [64]
CK [6]
SCK [64]
SCK
KSG
Key
Stream
IV [35]

FIG. 3

INTERNATIONAL SEARCH REPORT

Intern nal Application No
PCT/EP 00/07692

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 10605 A (NOKIA MOBILE PHONES LTD ;NOKIA MOBILE PHONES INC (US)) 12 March 1998 (1998-03-12)	1-6, 9-11, 13-15
Y	page 3, line 28 - line 29 page 4, line 16 - line 30 page 6, line 21 - line 23 page 7, line 14 - line 18 page 8, line 15 - line 21 page 11, line 4 -page 12, line 9 page 15, line 12 - line 14 page 31, line 23 - line 25 page 28, line 16 - line 19	7,8
Y	GB 2 327 567 A (ORANGE PERSONAL COMM SERV LTD) 27 January 1999 (1999-01-27) page 14, line 8 -page 15, line 7	7,8

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 December 2000	27/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Palencia Gutiérrez,C

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr. nal Application No
PCT/EP 00/07692

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9810605 A	12-03-1998	AU 4164297 A	26-03-1998
		BR 9711992 A	24-08-1999
		CN 1235740 A	17-11-1999
GB 2327567 A	27-01-1999	AU 8348798 A	10-02-1999
		CN 1264521 T	23-08-2000
		EP 0997047 A	03-05-2000
		WO 9904583 A	28-01-1999